Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2014 Proceedings | Southern (SAIS)

4-14-2014

DEVELOPMENT OF A DIGITAL FORENSICS LAB TO SUPPORT ACTIVE LEARNING

Kevin Floyd
Middle Georgia State College, kevin.floyd@mga.edu

Johnathan Yerby
Middle Georgia State College, johnathan.yerby@mga.edu

DEVELOPMENT OF A DIGITAL FORENSICS LAB TO SUPPORT ACTIVE LEARNING

Kevin S. Floyd
Middle Georgia State College
kevin.floyd@mga.edu

Johnathan Yerby
Middle Georgia State College
johnathan.yerby@mga.edu

ABSTRACT

The curriculum of a program in Information technology must be current and competitive to remain relevant and valuable. The purpose of this paper was to explore the benefits of digital forensics related to student active learning opportunities. The paper also used the widely accepted learning theories of active learning and constructivism to assist in the decision to build a hands-on digital forensics lab environment. An explanation of the processes, opportunities, challenges, and outcomes are available in the Lab design section. Finally the paper concludes with implications for students and recommendations for other higher education institutions that are considering enhancing theory with practical hands-on learning opportunities.

Keywords

Information Technology, Lab, Digital Forensics, Security, Constructivism, Experiential learning

INTRODUCTION

Digital forensics is a fairly new field that combines information technology, information security, investigations, criminal justice, and law enforcement (Caloyannides, 2001). Computer forensics investigations are generally conducted in four distinct steps; acquisition, identification, evaluation, and admission as evidence which would allow the results of the investigation to be admissible into court (Pollitt, 2007). In the report from the First Digital Forensic Research Workshop (FDFRW) (Palmer, 2001) digital forensics was divided into the following three areas; Law enforcement, Military Operations, and Business with the following primary objectives of prosecution, continuity of operations, and availability of service. The second and third areas have a secondary goal of prosecution, but they are concerned with attacks in real-time, but law enforcement is most often prosecuting after the event. At the 2001 FDFRWthe group defined digital forensics as:

> "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." (Palmer, 2001)

Cybersecurity and digital forensics is a growing field in the United States as cyber-attacks happen faster, more often, and cost more organizations like the National Security Agency, Department of Homeland Security, Federal Bureau of Investigations, U.S. Military, and numerous private firms seeking to protect, discover, and defend against security breaches.

Funding to create the digital forensics lab was supported by a National Science Foundation (NSF) grant to create the Advanced Cybersecurity Education (ACE) Consortium. The ACE Consortium consists of colleges in Florida, Georgia, South Carolina, and North Carolina. Operational goals of the NSF grant include developing and disseminating quality training and educational materials and implement educational technologies to support cyberforensic courses. XYZ State College, the lead institution in Georgia used $20,000 of ACE Consortium funding to create a digital forensics laboratory that will be used to accomplish operational goals of developing and disseminating training and educational materials while also allowing the institution to offer an additional scenario based advanced digital forensics course to students.

ACTIVE LEARNING

In recent years, there has been much debate in higher education about the traditional approach to teaching (Saulnier, et al., 2008; Wilson, 1995) and the active learning approach which emphasizes student engagement through activities related to the course topics (Bakke and Faley, 2007; Schiller, 2009; Williams and Chinn, 2009). Active learning is a broad term used to describe several different methods of instruction in which the learner is responsible for their own learning. Bonwell and Eison (1991) have contributed largely to the development of active learning and to its acceptance of a viable approach. Active learning includes practices such as group discussions, laboratory experiments, games, debates, and role play (Bonwell and Eison, 1991). Active learning uses problem-based learning. In a meta-analysis conducted by Vernon and Blake (1993),

student attitudes, class attendance, and student moods were found to be consistently more positive than those of students in courses that used only the traditional lecture approach to teaching and learning.

The idea that students learn best from active learning experiences has its roots in the constructivism learning theory. Constructivism learning theory originates from research by Dewey (1938), Piaget (1972), Vygotsky (1978),Ausubel (1968), and Bruner (1990). Under constructivism learning theory, the learner or student actively constructs information rather than passively receiving information from the environment. Knowledge is not simply transmitted from one person to another (Liu and Chen, 2010).

Vygotsky's (1978) theory of social constructivism focused on the interaction of learners with others in cognitive development. The constructivist perspective encourages learning through interaction (Tam, 2000). Through use of a lab environment instructors are able to apply concepts recognized as 'constructivist teachers' including:

- assess students' understanding through application and performance of open-structured tasks;
- encourage and accept student autonomy and initiative;
- use a wide variety of materials, including raw data, primary sources, and interactive materials and encourage students to use them;
- inquire about students' understandings of concepts before sharing his/her own understanding of those concepts;
- engage students in experiences that show contradictions to initial understandings and then encourage discussion;
- encourage student inquiry by asking thoughtful, open-ended questions and encourage students to ask questions to each other and seek elaboration of students' initial responses (Brooks and Brooks, 1993).

As fields like information systems and information technology have evolved, the addition of hands-on activities to support theoretical knowledge has become increasingly prevalent. According to the Association for Computing Machinery (ACM) Information Technology 2008 curriculum guidelines, "Information Technology is a laboratory discipline." A successful information technology program must not only teach students soft skills, but also technical skills or skills in understanding and modeling organizational processes and data, defining and implementing technical and process solutions, managing projects, and integrating systems within and across organizations and focusing on the application of information technology in helping individuals, groups, and organizations achieve their goals (Topi et al, 2010). The IS 2010 Curriculum Guidelines emphasizes the need for laboratories and access to specialized software to enable students to keep abreast of the rapidly changing technology environment and experience with facilities at least equivalent to those used in a typical organization operating within a program's domain (Topi et al., 2010).

There is a growing acceptance amongst academics on the value of supplementing theoretical knowledge with hands-on practical learning (Mengel& Bowling, 1995; Cigas, 2002; Aravena& Andres, 2009; Imboden&Strothmann, 2010). Duffy and Jonassen (1992) explained that a course curriculum can remain committed to theory-based instruction as a framework for thinking while simultaneously using a rich array of examples. Omrod (1995) indicated that course facilitators could encourage students' development by presenting class exercises that students can complete only with assistance. Learning only theory or only concentrating on specific hands-on exercises applicable now has the potential to result in only partial understandings and biased understandings. With traditional instruction, students are passive recipients of information (Prince, 2004). Theory is better understood when it can be practiced or applied. Active learning is also linked to higher levels of student engagement.

Research conducted by Floyd, Harrington, and Santiago (2009) suggested that when IT students exposed to active learning assignments, including hands-on lab exercises, student cognitive engagement or the integration and utilization of students' motivations and strategies in the course of their learning increased. The addition of the hands-on projects to enhance technical skills will only strengthen a student's ability to apply academic skills needed for an increasingly sophisticated workplace and society (Daggett, 2010).

DIGITAL FORENSICS IN HIGHER EDUCATION

In a recent study Symantec reported that cybercrime is costing the world $100 billion dollars every year (Symantec, 2012). With the rapidly growing number of computer crimes over the last decade including white-collar crime, violent-crime, terrorism, espionage, and pornography, criminal investigators and law enforcement agencies seek the expertise of digital forensic experts to inspect confiscated computer systems for evidence. (Srinivasan, 2013). Digital forensics is a relatively new and emerging academic discipline in information technology that involves the preservation, identification, extraction, and documentation of digital evidence in a format that can be presented in a court of law (Lunn, 2001).

With the need for more digital forensics professionals, there has been an increase in the number of higher education institutions that offer courses and programs in digital forensics as part of their information technology curriculum (Yasinsac & Manzano, 2001; Yasinsac, Erbacher, Marks, Pollitt, & Summer, 2003; Lim, 2006; Chi, 2009). In 2012, XYZ State College became a member of the Advanced Cyber Security Consortium (ACE) led by Daytona State College and funded by a National Science Foundation (NSF) grant. The goal of the consortium is to advance cyber forensic education in the southeastern United States. As a means of supporting this goal, the School of Information Technology at XYZ State has committed to the design, development, and implementation of a digital forensics lab to support and strengthen offerings in digital forensics education and training.

LAB DESIGN

The digital forensics laboratory was designed by a group of five senior capstone students. Two of the students in the group have previously taken an introduction to digital forensics course, while the remaining three students were enrolled in the introduction to forensics course while also working to create the new hands-on forensics lab. The students began with a needs analysis and decided that the lab should be capable of performing the following tasks:

- Establish categories for computer forensics tools
- Identify computer forensics category requirements
- Develop test assertions
- Identify test cases
- Establish a test method
- Report test results

A common trusted standard for maintaining the Forensic Software a main asset to the Digital Forensic Lab is the Daubert Standard (Hough, 1995):

- Whether the theory or technique in question can be and has been tested;
- Whether it has been subjected to peer review and publication;
- Its known or potential error rate;
- The existence and maintenance of standards controlling its operation;
- Whether it has attracted widespread acceptance within a relevant scientific community.

The hardware and software that was selected for the college's centralized digital forensics lab was:

Quantity	Hardware	Price	Lab Purpose
1	Samsung Galaxy Tablet 7" Display	$169.99	Showcase device for tablet media extraction.
10	23" HP Monitors	$2,140.00	Workstation Displays
2	Port and Cable Switches (DVI)	$305.38	Display Adapters
1	27" iMac Workstation	$2,946.98	Mac, OS X Scenarios
2	160GB Desktop IDE HD	$60.00	Legacy Data Storage
1	Samsung 840 SSD	$97.90	Data Storage (Scenarios involving the challenges digital forensic examiners face with SSDs)
2	X-Rays Forensics Guide	$99.38	Learning Material (Textbook)
5	Kingston 16GB Flash Card	$54.00	External Data Storage
1	WD Blue 320GB Mobile HDD	$46.99	Mobile Data Storage
5	WD Caviar Blue SATA 500GB HD	$275.30	Data Storage
1	Forensics Tower Computer	$8,267.00	Workstation For Advanced Scenarios
1	Desktop PC	DONATED	For Use As A Linux System
1	CRU WiebeTech Ditto	$1,649.00	Digital Forensics Field Kit
1	Tableau Full Kit	$454.00	Write Blocker (Prevents From Altering Files)
1	Ultradock v5	$199.00	Write Blocker (Advanced For Use With Multiple Devices)
1	Ultradock v4	$99.00	Write Blocker (Advanced For Use With Multiple Devices)

The lab hardware was $16,864 with plans to purchase software in the future as well as supportive technology that will allow a computer display to be shared wirelessly with the projector that is already installed in the room.

The next goal was to obtain licenses for software to be used with digital forensic tools. The following list includes the majority of the software suites that were needed by the digital forensics lab:

- Encase is a suite of digital forensic software, developed by Guidance Software. Encase specializes in data acquisition, analysis and reporting.
- FTK was developed by AccessData, and stands for Forensic Toolkit. FTK offers the ability to create duplicate disk images of a hard drive and to scan those images for various types of information; such as deleted files, text within a file, and specific file types.
- ProDiscover is similar to FTK in that it also offers investigators the ability to preserve data through disc images and it has search features that allow investigators to find hidden data on the hard drive.
- Cellebrite is used primarily for digital forensic investigations on mobile devices. Cellebrite offers numerous data extraction, transfer, and analysis tools for cellular phones and other mobile devices.
- Microsoft Office Suite,
- MS Windows 97, XP, 2000, 2003, Vista, 7, 2008, 8, & 2012
- Linux Systems (Mint & Ubuntu)
- Mac OS
- Programming Languages
- Specialized Viewers
- Open Office

After installing and configuring forensics workstations the students created scenarios using a fictional crime syndicate where students will use various digital forensics tools and techniques to conduct an investigation and report their findings. Students will adhere to the nine step model often used by law enforcement that consists of: Identification, Preparation, Approach Strategy, Preservation, Collection, Examination, Analysis, Presentation, and Returning Evidence (Reith, Carr, &Gunsch, 2002). The first scenario is an email investigation on a Windows 7 based machine with a user that has attempted to hide their actions by deleting emails, changing file extensions, and using multiple email accounts. The second scenario is an investigation on a Linux based OS that requires students to perform bit-stream copies, hashing, and rebuilding several multimedia files. The scenarios are designed without a prescribed set of steps of correct answers. Students will be required to think through complex problems, preserve the evidence, use the tools and software that is available, and justify their choices. The complex ill-structured nature of the problem is designed to allow students the freedom to explore a realistic situation that they may encounter when working in the field of digital forensics.

IMPLICATIONS

Adding the digital forensics lab will enable the college to offer at least one additional advanced forensics course to students and to non-degree seekers that wish to earn a certificate in Information Security. The digital forensics lab will be a valuable tool to train partner institutions such as technical colleges and high schools to increase their course offerings in digital forensics and attract more bright minds to the field of digital forensics and cybersecurity. The proposed lab supports collaboration between researchers, colleagues, and students. The facilitation of collaboration allows influential users to become champions and trainers of new technologies.

CONCLUSIONS

Cyber forensics is a rapidly growing field (Lunn, 2001) and is increasingly being taught within IT-related disciplines at institutions of higher education to train and prepare students to fill the growing number of jobs in the field (Yasinsac,

Erbacher, Marks, Pollitt, & Summer, 2003). The XYZ State College School of Information Technology was provided with the opportunity to enhance its course offerings in digital forensics with the help of an NSF grant. As part of a senior capstone course project, a group of students worked collaboratively with IT faculty to design and develop a forensics lab. During the design process, students consulted with professionals in digital forensics such as local law enforcement agencies, and the Georgia Bureau of Investigation to help ensure that the lab would closely simulate what they may encounter when working in the field of digital forensics. The lab will enable future IT students to engage in active learning in the area of digital forensics while also being exposed to important theoretical concepts.

REFERENCES

1. ACM. (2008). Information technology 2008: Curriculum guidelines for undergraduate degree programs in information technology. http://www.acm.org/education/curricula/IT2008%20Curriculum.pdf
2. Aravena M, & Andres, R. (2009). Use of a remote network lab as an aid to support teaching computer. *CLEI Electronic Journal*, *12*(1), 8.
3. Ausubel, D. (1968). *Educational psychology: A cognitive view*. New York: Holt, Rinehart & Winston.
4. Bakke, S. &Faley, R.H. (2007). A student-centric approach to large introductory IS survey courses. *Journal of Information Systems Education*, *18*(3), 321-328.
5. Bonwell, C.C. &Eison, J.A. (1991). *Active learning: Creating excitement in the classroom*.ASHE-ERIC Higher Education Report No. 1. Washington, D.C.: The George Washington University, School of Education and Human Development.
6. Brooks, J. G. and Brooks, M. G. (1993). *In search of understanding: the case for constructivist classrooms*, Alexandria, VA: American Society for Curriculum Development.
7. Bruner, J. (1990). Acts of Meaning. Cambridge, MA: Harvard University Press.
8. Caloyannides, M. A. (2001). *Computer Forensics & Privacy*. Artech House Publishers.
9. Chi, H. (2009). Design and implementation of a digital forensics lab: A case study for teaching digital forensics to undergraduate students. Retrieved December 15, 2013 from http://www.famu.edu/cis/year2009-Chi-Jones-etal-CATE.pdf.
10. Cigas, J. (2002). A computer networking laboratory for administration and networking.*Frontiers in Education*, *1*(T3D), 12-11.
11. Daggett, W. (2010). Preparing students for their technological future. International Center for Leadership in Education, Retrieved from http://www.leadered.com/pdf/Preparing Students for Tech Future white paper.pdf
12. Dewey, J. (1938). Experience and education. New York: Macmillan.
13. Duffy, T. M., &Jonassen, D. H. (1992). *Constructivism and the technology of instruction: a conversation*. (Thomas M Duffy & David H Jonassen, Eds.)*Computers in Human Behavior* (Vol. In Press,, p. 221). Lawrence Erlbaum Associates. Retrieved from http://books.google.com/books?id=7Uv8NHvKK44C
14. Hough, J. (1995). Recovered Memories of Childhood Sexual Abuse: Applying the Daubert Standard in State Courts. *S. Cal. L. Rev.*, 69, 855.
15. Floyd, K.S., Harrington, S.J., & Santiago, J. (2009). Improving I.S. student engagement and perceived course value. Proceedings of the 2009 Southern Association for Information Systems Conference, 24-29.
16. Imboden, T., &Strothmann, D. (2010). Design and implementation of a low-cost networking and voip lab for undergraduate networking curriculum instruction. *Issues in Information Systems*, *11*(2), 1-6. Retrieved from http://iacis.org/iis/2010/1-6_LV2010_1433.pdf
17. Lim, N. (2006). Crime investigation: A course in computer forensics. *Communications of AIS*, *18*(10), 2-34.
18. Liu, C.C., & Chen, I. J. (2010). Evolution of constructivism. *Contemporary Issues in Education Research*, *3*(4), 63-66.
19. Lunn, D. (2001). Computer forensics: An overview. SANS Institute. Retrieved from http://www.giac.org/paper/gsec/559/computer-forensics-overview/101340.
20. Mengel, S. A., & Bowling, C. D. (1995). Supporting networking courses with a hands-on laboratory. *Frontiers in Education Conference, 1995.Proceedings., 1995* (Vol. 2, p. 4c2.20–4c2.23 vol.2). Presented at the Frontiers in Education Conference, 1995.Proceedings., 1995. doi:10.1109/FIE.1995.483214
21. Omrod, J. (1995). *Educational Psychology: principles and applications*, Englewood Cliffs, NJ: Prentice Hall.
22. Palmer, G. (2001). *A road map for digital forensic research*.(DFRWS technical report).Retrieved from http://www.dfrws.org/2001/dfrws-rm-final.pdf

23. Piaget, J. (1972). The psychology of the child. New York: Basic Books.
24. Pollitt, M. M. (2007, April). An ad hoc review of digital forensic models. In *Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on* (pp. 43-54). IEEE.
25. Prince, M. (2004). Does active learning work? A review of the research. *Journal of Engineering Education*, *93*(3), 223-231.
26. Reith, M., Carr, C., &Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3), 1-12.
27. Saulnier, B.M., Landry, J.P., Longenecker Jr., H.E., & Wagner, T.A. (2008). From teaching to learning: Learning-centered teaching and assessment in information systems education. *Journal of Information Systems Education*, *19*(2), 169-174.
28. Schiller, S.Z. (2009). Practicing learner-centered teaching: Pedagogical design and assessment of a Second Life project. *Journal of Information Systems Education*, *20*(3), 369-381.
29. Srinivasan, S. (2013). Digital forensics curriculum in security education. *Journal of Information Technology Education: Innovations in Practice*, *12*, 147-157.
30. Tam, M. (2000). Constructivism, instructional design, and technology: Implications for transforming distance learning. *Educational Technology & Society*, *3*(2), Retrieved from http://www.ifets.info/journals/3_2/tam.html
31. Topi, H., Valacich, J.S., Wright, R.T., Kaiser, K.M., Nunamaker, J.F., Sipior, J.C., de Vreede, G.J. (2010). IS 2010: Curriculum guidelines for undergraduate degree programs in information systems. Retrieved from http://www.acm.org/education/curricula/IS%202010%20ACM%20final.pdf.
32. Vernon, D., & Blake, R. (1993). Does problem-based learning work? A meta-analysis of evaluation research. *Academic Medicine*, *68*(7), 550-563.
33. Vygotsky, L.S. (1978). Mind and society: The development of higher mental processes. Cambridge, MA: Harvard University Press.
34. Williams, J. & Chinn, S.J. (2009). Using Web 2.0 to support t the active learning experience. *Journal of Information Systems Education*, *20*(2), 165-174.
35. Wilson, B. (1995). Metaphors for instruction: Why we talk about learning environments. Educational Technology, *35*(5), 25-30.
36. Yasinsac, A., Erbacher, R.F., Marks, D.G., Pollitt, M.M., & Sommer, P.M. (2003). Computer forensics education, *IEEE Computer Security and Privacy Magazine*, *1*(4), 15-23.
37. Yasinsac, A., &Manzano, Y. (2001). Policies to enhance computer and network forensics.*Proceedings of IEEE Workshop on Information Assurance and Security*, Westpoint, NY, June.http://www.cs.fsu.edu/~yasinsac/papers/my01.pdf
38. *2012 norton study: Consumer cybercrime estimated at $110 billion annually*. (2012, 12 05). Retrieved from http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02